COURSE OVERVIEW IT0011

ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)

Course Title

ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)

Course Date/Venue

February 02-06, 2025/TBA Meeting Room,
The Tower Plaza Hotel, Dubai, UAE

Course Reference

IT0011

Course Duration/Credits

Five days/3.0 CEUs/30 PDHs

Course Description

This practical and highly-interactive course includes real-life case studies and exercises where participants will be engaged in a series of interactive small groups and class workshops.

This course is designed to provide participants with a detailed and up-to-date overview of ISO 27001 Risk Assessment. It covers the importance, standard key concepts and principles of risk management; the organizational context and the internal and external factors affecting information security; the roles and responsibilities for risk assessment and the importance of leadership commitment and support; the risk assessment framework, asset identification and valuation; and the common threats to information security and vulnerabilities in information systems.

During this interactive course, participants will learn the risk identification techniques, risk assessment methodologies and risk assessment tools; the risk analysis process, risk impact assessment, risk likelihood assessment, risk evaluation criteria and risk prioritization; the organization's risk appetite and tolerance; aligning the assessment with risk appetite; the risk treatment options and developing a risk treatment plan; selecting information security controls, applying residual risks management and integrating risk treatment with ISMS; establishing a process for ongoing risk monitoring and reviewing and updating the risk assessment regularly; the performance measurement and metrics; the internal and external audits; and the continual improvement practices.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain an in-depth knowledge on information security, cybersecurity and privacy protection risk assessment in accordance with ISO 27001 standard
- Discuss the importance, key concepts and principles of risk management
- Explain the organizational context and the internal and external factors affecting information security
- Discuss the roles and responsibilities for risk assessment and the importance of leadership commitment and support
- Develop a risk assessment framework as well as apply asset identification and valuation
- Identify the common threats to information security and vulnerabilities in information systems
- Apply risk identification techniques, risk assessment methodologies and risk assessment tools
- Carryout risk analysis process, risk impact assessment, risk likelihood assessment, risk evaluation criteria and risk prioritization
- Define the organization's risk appetite and tolerance as well as align the assessment with risk appetite
- Discuss risk treatment options and develop a risk treatment plan
- Select information security controls, apply residual risks management and integrate risk treatment with ISMS
- Establish a process for ongoing risk monitoring and review and update the risk assessment regularly
- Apply performance measurement and metrics, conduct internal and external audits and implement continual improvement practices

Exclusive Smart Training Kit - H-STK®

*Participants of this course will receive the exclusive "Haward Smart Training Kit" (**H-STK**®). The **H-STK**® consists of a comprehensive set of technical content which includes **electronic version** of the course materials, sample video clips of the instructor's actual lectures & practical sessions during the course conveniently saved in a **Tablet PC**.*

Who Should Attend

This course provides an overview of all significant aspects and considerations of ISO 27001 risk assessment for information security managers, IT professionals, compliance officers, risk managers, internal auditors, data protection officers (DPOs), business continuity managers, senior management, consultants, and anyone involved in the development or implementation of an ISMS.

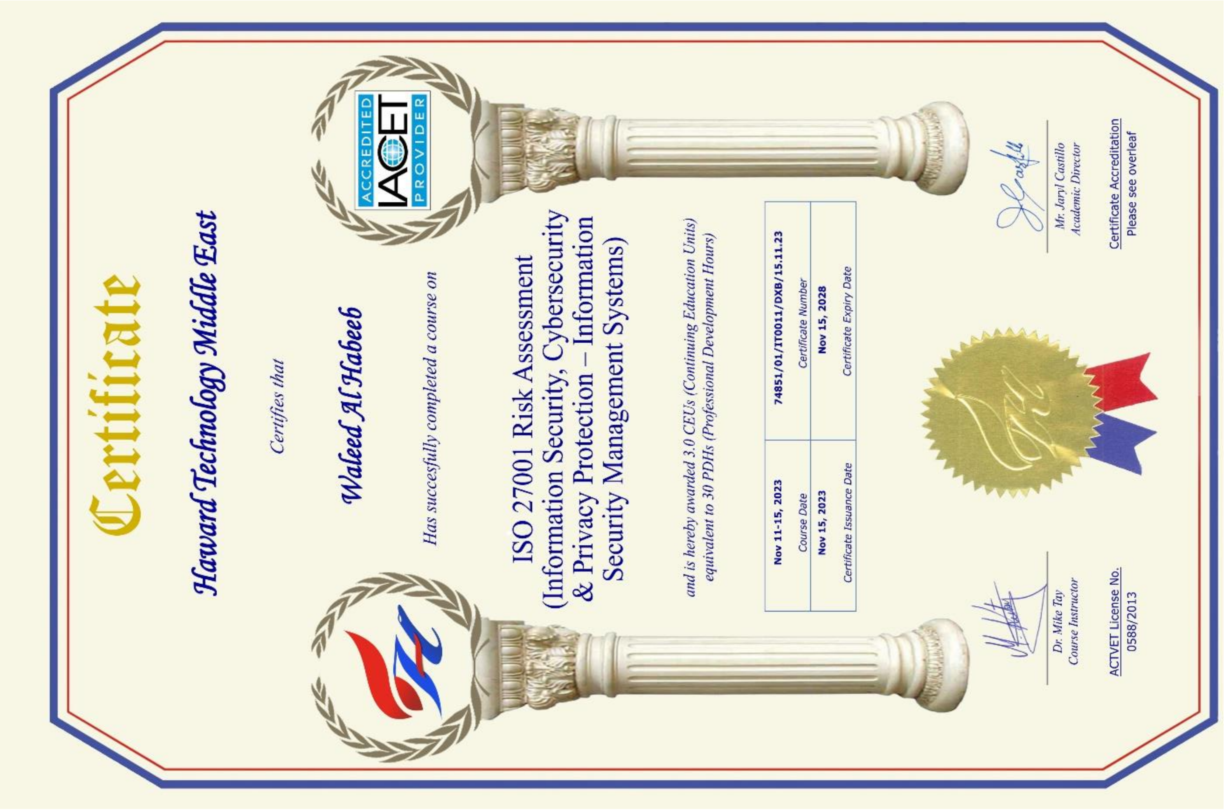
Course Certificate(s)

(1) Internationally recognized Competency Certificates and Plastic Wallet Card Certificates will be issued to participants who completed a minimum of 80% of the total tuition hours and successfully passed the exam at the end of the course. Certificates are valid for 5 years.

Recertification is FOC for a Lifetime.

Sample of Certificates

The following are samples of the certificates that will be awarded to course participants:-



Certificate

Haward Technology Middle East

Certifies that

Waleed Al Habeeb

Has succesfully completed a course on

ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)

and is hereby awarded 3.0 CEUs (Continuing Education Units) equivalent to 30 PDHs (Professional Development Hours)

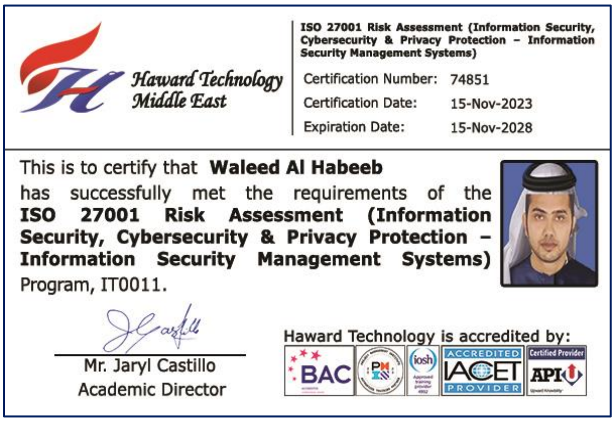
Nov 11-15, 2023 Course Date	**74851/01/IT0011/DXB/15.11.23** Certificate Number
Nov 15, 2023 Certificate Issuance Date	**Nov 15, 2028** Certificate Expiry Date

Dr. Mike Tay
Course Instructor

Mr. Jaryl Castillo
Academic Director

ACTVET License No.
0588/2013

Certificate Accreditation
Please see overleaf



Haward Technology Middle East

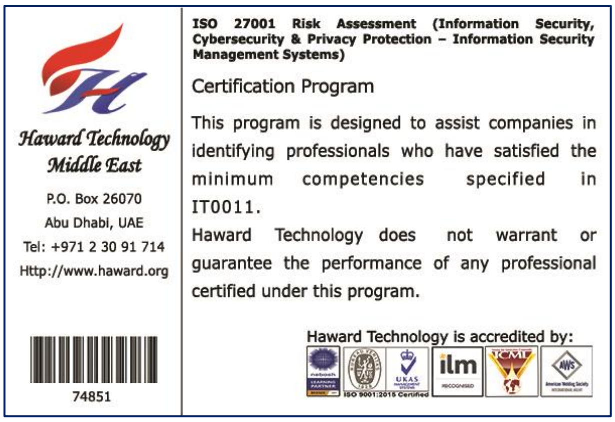
ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)

Certification Number:	74851
Certification Date:	15-Nov-2023
Expiration Date:	15-Nov-2028

This is to certify that **Waleed Al Habeeb** has successfully met the requirements of the **ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)** Program, IT0011.

Mr. Jaryl Castillo
Academic Director

Haward Technology is accredited by:



Haward Technology Middle East

P.O. Box 26070
Abu Dhabi, UAE
Tel: +971 2 30 91 714
Http://www.haward.org

74851

ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)

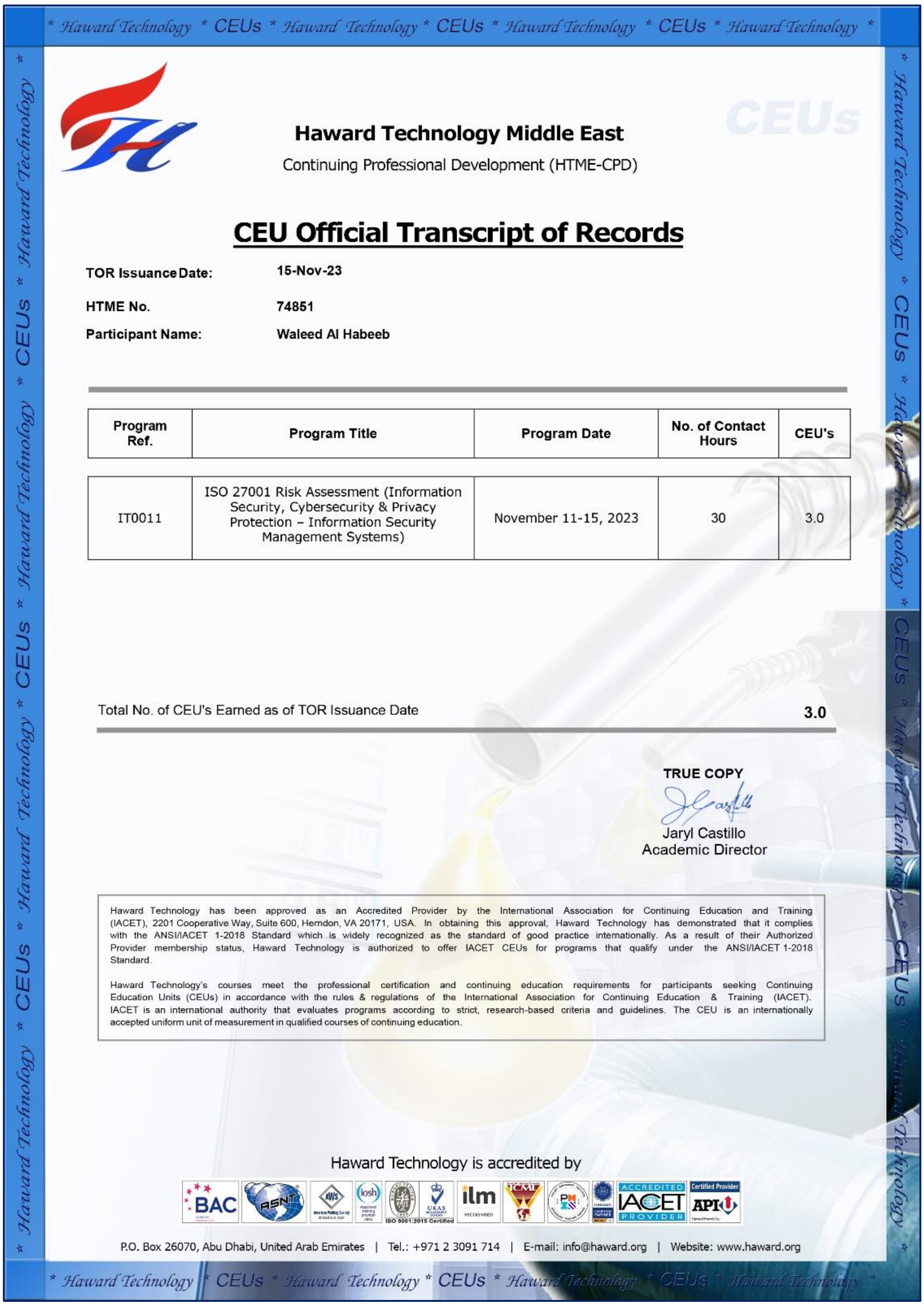
Certification Program

This program is designed to assist companies in identifying professionals who have satisfied the minimum competencies specified in IT0011.

Haward Technology does not warrant or guarantee the performance of any professional certified under this program.

Haward Technology is accredited by:

(2) Official Transcript of Records will be provided to the successful delegates with the equivalent number of ANSI/IACET accredited Continuing Education Units (CEUs) earned during the course.



Haward Technology Middle East

Continuing Professional Development (HTME-CPD)

CEU Official Transcript of Records

TOR Issuance Date:	**15-Nov-23**
HTME No.	**74851**
Participant Name:	**Waleed Al Habeeb**

Program Ref.	**Program Title**	**Program Date**	**No. of Contact Hours**	**CEU's**
IT0011	ISO 27001 Risk Assessment (Information Security, Cybersecurity & Privacy Protection – Information Security Management Systems)	November 11-15, 2023	30	3.0

Total No. of CEU's Earned as of TOR Issuance Date **3.0**

TRUE COPY

Jaryl Castillo
Academic Director

Haward Technology has been approved as an Accredited Provider by the International Association for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this approval, Haward Technology has demonstrated that it complies with the ANSI/IACET 1-2018 Standard which is widely recognized as the standard of good practice internationally. As a result of their Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for programs that qualify under the ANSI/IACET 1-2018 Standard.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking Continuing Education Units (CEUs) in accordance with the rules & regulations of the International Association for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology is accredited by

P.O. Box 26070, Abu Dhabi, United Arab Emirates | Tel.: +971 2 3091 714 | E-mail: info@haward.org | Website: www.haward.org

Certificate Accreditations

Certificates are accredited by the following international accreditation organizations: -

- The International Accreditors for Continuing Education and Training (IACET - USA)

  Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

  Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

  Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

- British Accreditation Council (BAC)

  Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

Course Fee

US$ 5,500 per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

Dr. Mike Tay, PhD, MSc, BSc, is a **Senior IT**, **Telecommunications**, **Control & Electronics Engineer** with over **35 years** of extensive experience. His expertise widely covers in the areas of **Cloud Infrastructure**, **Digital Transformation**, **Cloud Security Mechanism**, **E-Communication & Collaboration** Skills, **Virtual Communication**, **Social Networking**, **Business Intelligence** Tools, **IT Disaster Recovery & Planning**, **IT Risk Management** Concepts, **IT Risk Management** Standard Approaches, **IT Risk Management** Planning, **IT Risk** Identification, **IT Risk Monitoring** & **Control**, **Information Technology** Architectures, **Application** Architecture, **Portfolio** Management, **Application Security**, **Application Integration** Technologies & Strategies, **Solution Architecture** Patterns, **Web Applications** & Services, **Mobile** & **Cloud Applications**, **Blended Learning** Programs, **Web Programming**, Advanced **Database Management** Systems, **Web Design**, **HCI**, 3D Animation, Multimedia Design, Gamification Techniques, Internal & External Auditing, **OS Architectures** and **Network Security**. Further, he is also well-versed in Mobile Protocols, 4G LTE, GSM/UMTS, CMDA2000, WIMAX Technology, HSPA+, Alarm Management System, Computer Architecture, Logic & Microprocessor Design, Embedded Systems Design plus Computer Networking with CISCO, Network Communication, Industrial Digital Communication, Designing Telecommunications Distribution System, Electrical Engineering, WiMAX Broadband Wireless System, TT Intranet & ADSL Network, TT Web & Voicemail, Off-site ATM Network, IT Maintenance, Say2000i, IP Phone, National Address & ID Automation, Electricity Distribution Network, Customs Network & Maintenance, LAN & WAN Network, UYAP Network, Network Routing Protocols, Multicast Protocols, Network Management Protocols, Mobile & Wireless Networks and Digital Signal Processing. Currently, he is the **Technical Advisor** of **Izmir Altek**.

During his career life, Dr. Tay worked with various companies such as the **KOC Sistem**, **Meteksan Sistem**, **Altek BT**, **Yasar University**, **Dokuz Eylul University**, **METU** and occupied significant positions like the **Aegean Region Manager**, **Group Leader**, **Technical Services Manager**, **Field Engineer**, **Research Assistant**, **Instructor**, **Technical Advisor** and the **Dr. Instructor**.

Dr. Tay has **PhD**, **Master** and **Bachelor** degrees in **Electrical & Electronic Engineering** from the **Dokuz Eylul University** and the **Middle East Technical University** (**METU**) respectively. Further, he is a **Certified Instructor/Trainer**, **Technical Trainer (Australia)**, **Trainer** for **Data-Communication System (England & Canada)**, a **Certified Internal Verifier/Assessor/Trainer** by the **Institute of Leadership & Management** (**ILM**), a **Certified CISCO** (**CCSP**, **CCDA**, **CCNP**, **CCNA**, **CCNP**) **Specialist**, a **Certified CISCO IP Telephony Design Specialist**, **CISCO Rich Media Communications Specialist**, **CISCO Security Solutions** & **Design Specialist** and **Information Systems Security** (**INFOSEC**) **Professional**. He has delivered and presented innumerable training courses and workshops worldwide.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30%	Lectures
20%	Practical Workshops & Work Presentations
30%	Hands-on Practical Exercises & Case Studies
20%	Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1: Sunday, 02nd of February 2025

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 – 0930	***Overview of ISO 27001*** *Introduction to ISO 27001 Standard • Key Principles and Benefits of Implementing an Information Security Management System (ISMS)*
0930 – 0945	*Break*
0945 – 1045	***Understanding Risk Management*** *Definition and Importance of Risk Management • Key Concepts and Principles of Risk Management*
1045 – 1145	***Information Security Risk Assessment Overview*** *Purpose and Scope of Risk Assessment • Relationship Between Risk Assessment and ISO 27001*
1145 – 1230	***Establishing the Context*** *Understanding the Organizational Context • Identifying Internal and External Factors Affecting Information Security*
1230 – 1245	*Break*
1245 – 1330	***Roles & Responsibilities*** *Defining Roles and Responsibilities for Risk Assessment • Importance of Leadership Commitment and Support*
1330 – 1420	***Developing a Risk Assessment Framework*** *Key Components of a Risk Assessment Framework • Steps for Establishing an Effective Framework*
1420 – 1430	***Recap***
1430	*Lunch & End of Day One*

Day 2: Monday, 03rd of February 2025

0730 – 0830	***Asset Identification & Valuation*** *Identifying Information Assets • Valuing Assets Based on their Importance to the Organization*
0830 – 0930	***Identifying Threats*** *Common Threats to Information Security • Techniques for Identifying Threats*
0930 – 0945	*Break*

0945 – 1200	***Identifying Vulnerabilities*** *Common Vulnerabilities in Information Systems • Techniques for Identifying Vulnerabilities*
1200 – 1230	***Risk Identification Techniques*** *Qualitative vs. Quantitative Approaches • Tools and Techniques for Risk Identification*
1230 – 1245	*Break*
1245 – 1330	***Risk Assessment Methodologies*** *Overview of Different Risk Assessment Methodologies (e.g., OCTAVE, NIST, ISO 27005) • Selecting an Appropriate Methodology for the Organization*
1330 – 1420	***Risk Assessment Tools*** *Software and Tools for Conducting Risk Assessments • Features and Benefits of Different Tools*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Two*

Day 3: **Tuesday, 04th of February 2025**

0730 – 0830	***Risk Analysis Process*** *Steps for Analyzing Identified Risks • Qualitative vs. Quantitative Risk Analysis*
0830 – 0930	***Risk Impact Assessment*** *Assessing the Potential Impact of Risks • Techniques for Impact Assessment*
0930 – 0945	*Break*
0945 – 1100	***Risk Likelihood Assessment*** *Assessing the Likelihood of Risk Occurrence • Techniques for Likelihood Assessment*
1100 – 1230	***Risk Evaluation Criteria*** *Establishing Criteria for Risk Evaluation • Evaluating Risks Based on Impact and Likelihood*
1230 – 1245	*Break*
1245 – 1330	***Risk Prioritization*** *Prioritizing Risks for Treatment • Techniques for Risk Prioritization*
1330 – 1420	***Risk Appetite & Tolerance*** *Defining the Organization's Risk Appetite and Tolerance • Aligning Risk Assessment with Risk Appetite*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Three*

Day 4: **Wednesday, 05th of February 2025**

0730 – 0830	***Risk Treatment Options*** *Overview of Risk Treatment Options (Avoidance, Mitigation, Transfer, Acceptance) • Selecting Appropriate Treatment Options for Identified Risks*
0830 – 0930	***Developing a Risk Treatment Plan*** *Creating a Comprehensive Risk Treatment Plan • Assigning Responsibilities and Timelines*
0930 – 0945	*Break*
0945 – 1100	***Selecting Information Security Controls*** *Overview of ISO 27001 Annex A Controls • Selecting and Implementing Appropriate Controls*
1100 – 1230	***Residual Risk Management*** *Assessing and Managing Residual Risks • Techniques for Monitoring Residual Risks*

1230 – 1245	*Break*
1245 – 1330	***Integrating Risk Treatment with ISMS*** *Aligning Risk Treatment with ISMS Objectives • Continuous Monitoring and Improvement*
1330 – 1420	***Case Studies & Best Practices*** *Reviewing Real-World Examples of Risk Treatment • Discussing Best Practices in Risk Management*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Four*

Day 5: Thursday, 06th of February 2025

0730 – 0930	***Risk Monitoring & Review*** *Establishing a Process for Ongoing Risk Monitoring • Reviewing and Updating the Risk Assessment Regularly*
0930 – 0945	*Break*
0945 – 1030	***Performance Measurement & Metrics*** *Defining Key Performance Indicators (KPIs) for Risk Management • Measuring and Evaluating Risk Management Performance*
1030 – 1115	***Internal & External Audits*** *Preparing for Risk Management Audits • Conducting Internal and External Audits*
1230 – 1245	*Break*
1245 – 1300	***Continual Improvement in Risk Management*** *Identifying Opportunities for Improvement • Implementing Continual Improvement Practices*
1300 – 1315	***Course Conclusion***
1315 – 1415	***COMPETENCY EXAM***
1415 – 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

Practical Sessions

This practical and highly-interactive course includes real-life case studies and exercises:-

Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org